

## WHAT IS CLAIMED IS:

1           1. A method for collecting and analyzing first data on a first communication line  
2 comprising the steps of:

- 3           (a) receiving the first data from the first communication line;  
4           (b) segregating the first data into packets;  
5           (c) selecting packets based on a respective first characteristic of each packet;  
6           (d) associating a respective index with each of the selected packets;  
7           (e) converting each of the selected packets into a respective record including its  
8 respective index;  
9           (f) storing the records;  
10          (g) storing a count based on a respective second characteristic of each of the  
11 selected packets received during each of a plurality of successive periods.

1           2. A method for monitoring data on a first communication line comprising:  
2 receiving the data from the first communication line;  
3 extracting a plurality of packets from the received data; and  
4 recursively generating statistics corresponding to the plurality of packets.

1           3. A method for collecting and analyzing first data transmitted on a first  
2 communication line comprising the steps of:

- 3           (a) receiving the first data from the first communication line;  
4           (b) segregating the first data into packets;  
5           (c) selecting packets based on a respective type of each packet;  
6           (d) associating a respective index with each of the selected packets;  
7           (e) converting each of the selected packets into a respective record including its  
8 respective index;  
9           (f) storing the records;  
10          (g) receiving a first duration value corresponding to a first time period;  
11          (h) generating at least one statistic corresponding to packets received during each  
12 successive first time periods; and  
13          (i) storing the value of at least one statistic for a plurality of successive time  
14 periods.

1           4.       The method according to claim 3 further comprising the step of generating  
2 a further statistic using at least one of the stored records and the stored at least one  
3 statistic.

1           5.       The method according to claim 3 further comprising the steps of:  
2 receiving a second duration value corresponding to a second time period longer  
3 than the first time period; and  
4 generating a further statistic corresponding to packets received during the second  
5 time period encompassing at least one first time period using at least one of the stored  
6 records and the stored at least one statistic.

1           6.       The method according to claim 3 wherein the at least one statistic includes  
2 at least one of a number of bits, a number of bytes, a number of packets, a number of  
3 packets of a predetermined protocol, a number of packets of a predetermined protocol  
4 layer, a number of packets having a predetermined source address, and a number of  
5 packets having a predetermined destination address of a respective packet.

1           7.       The method according to claim 3 wherein a record includes a portion of its  
2 respective packet plus its respective index.

1           8.       The method according to claim 3 wherein the respective index of a packet  
2 corresponds to a time when the packet was received.

1           9.       A method according to claim 8 further comprising the steps of receiving a  
2 time signal from a global positioning satellite indicating an absolute time and generating  
3 the time when a packet was received based on the absolute time.

1           10.      A method according to claim 3 wherein the received packets originated  
2 from a second communication line and each received packet includes an indication of a  
3 respective first time corresponding to its transmission on the second communication line,  
4 the method further comprising:

5 determining a respective second time when each packet is received from the first  
6 communication line; and

7 generating a transmission delay corresponding to each packet by subtracting its  
8 respective second time from its respective first time.

1           11.      A method according to claim 10 wherein the transmission delay  
2 corresponding to each packet is calculated based on a time the packet is detected on a first

link, a time the packet is detected on a second link, a rate of data transmission on the first link, and a length of the packet on the first link.

12. The method according to claim 3 wherein step (a) includes receiving the first data from the first communication line using a non-intrusive coupling to the first communication line.

13. The method according to claim 3 further comprising the step of receiving information indicating at least one of a type of packets to be selected in step (c), the first duration value, and an identification of which statistics to generate in step (h).

14. The method according to claim 13 wherein the information is received via the first communication line.

15. Canceled.

16. A method according to claim 10 including the step of receiving a time signal from a global positioning satellite for determining the second time.

17. A method according to claim 3 wherein step (h) includes generating at least one quality of service value for each successive time period corresponding to packets of a predetermined packet type received during each respective successive time period.

18. A method according to claim 17 wherein the at least one quality of service value indicates at least one of a round trip delay and a retransmit rate corresponding to the packets of the predetermined packet type received during the respective successive time period.

19. A method according to claim 3 wherein step (c) includes determining a respective type of each packet based on at least one of a corresponding application type, a corresponding packet content, a packet source, and a packet destination.

20. A method according to claim 3 wherein the first communication line is in a network including a user and step (h) includes generating at least one user profiling statistic for each successive time period corresponding to packets destined to or from a user which are received during each respective successive time period.

21. A method according to claim 20 wherein the at least one user profiling statistic is generated using the records stored in the memory.

1           22. A method according to claim 3 further comprising the step of receiving an  
2 input from a user identifying a user statistic and step (h) includes generating the user  
3 statistic.

1           23. A method according to claim 3 further comprising the steps of:  
2 receiving an input from a user identifying a user statistic; and  
3 generating the user statistic using at least one of the stored statistics and the stored  
4 records.

1           24. A method according to claim 3 wherein the first data is transmitted on the first  
2 communication line according to a first protocol, the method further comprising the step of  
3 receiving decoding parameters corresponding to the first protocol and step (a) includes  
4 receiving the first data according to the decoding parameters and step (b) includes  
5 segregating the received first data into packets according to the decoding parameters.

1           25. A method according to claim 3 wherein  
2 step (h) includes generating a separate count for each of a plurality of packet types  
3 corresponding to a number of packets of each respective one of the plurality of packet  
4 types received during each respective successive time period; and the method further  
5 comprises the step of

6 displaying the plurality of packet types and their corresponding statistics  
7 accumulated over a second time period greater than the first time period in a first portion  
8 of a display area of a display device;

1           26. A method according to claim 25 wherein the plurality of packet types are  
2 selectable by a user and the method further comprises the steps of:  
3 receiving a user selection of one of the packet types by a user;  
4 displaying statistics corresponding to packets of the selected packet type received  
5 during the second time period.

1           27. A method according to claim 25 further comprising the step of graphically  
2 displaying the statistics corresponding to the plurality of packet types in a plot over the  
3 second time period in a second portion of the display area.

1           28. A method according to claim 25 further comprising the step of:

generating a graphical display of the statistics corresponding to the plurality of packet types in a plot ranging over the second time period in a second portion of the display area, wherein the plot includes a plurality of discrete selectable time periods; receiving a user selection of a range of the plurality of discrete selectable time periods; updating the graphical display to display statistics corresponding to the selected time periods.

29. A method according to claim 3 further comprising the steps of:

identifying packets belonging to a data stream; storing stream identification information as one of a separate record and a separate field in the records corresponding to the identified packets.

30. A method according to claim 29 further comprising the step of recreating the data stream using the stored records and the stored stream identification information.

31. A method according to claim 3 wherein

the first communication line is in a network including a second communication line,

step (d) includes determining a respective time value corresponding to a time when each of the selected packets was received and the respective index associated with each selected packet includes its respective time value,

and step (e) includes converting each of the selected packets into a respective record which includes a uniquely identifiable portion of the respective selected packet;

and the method further comprises the steps of:

receiving second data from the second communication line;

segregating the second data into packets;

determining a respective type of each packet received from the second communication line;

selecting packets received from the second communication line based on their respective type;

determining a respective time when each of the selected packets received from the second communication line was received;

18 associating a respective index with each of the selected packets received from the  
19 second communication line, the respective index corresponding to a time when the packet  
20 was received from the second communication line;

21 convert each of selected packets received from the second communication line into  
22 a respective record that includes a uniquely identifiable portion the selected packet from  
23 the second communication line and includes its respective index;

24 storing the records corresponding to the selected packets received from the second  
25 communication line in a third memory;

26 comparing the uniquely identifiable portions of packets in records stored in the  
27 memory to those in records stored in the third memory to determine which selected  
28 packets received from the first communication line correspond to packets received from  
29 the second communication line to generate matched pairs of packets;

30 generating a transmission delay corresponding to each matched pair of packets  
31 using their respective indexes.

1 32. The method according to claim 31 wherein the transmission delay for a  
2 particular matched packet is calculated based on a time of receipt of the matched packet on  
3 the first transmission line, a time of receipt of the matched packet on the second  
4 transmission line, a rate of data transmission on the first transmission line, and a length of  
5 the matched packet on the first transmission line.

1 33. A method according to claim 32 wherein the first communication line  
2 transmits data using a first protocol and the second communication line transmits data  
3 using a second protocol different from the first protocol.

1 34. A method according to claim 31 wherein the transmission delay is  
2 generated at a level of accuracy less than 10 microseconds.

1 35. A method for routing first data from a first point to a second point in a  
2 communication network including a plurality of paths between the first point and the  
3 second point, the method comprising the steps of:

4 generating flow statistics based on the flow of second data on the plurality of paths  
5 between the first point and the second point, the second data being separate from the first  
6 data;

7 routing the first data between the first and second points based on the generated  
8 flow statistics.

1 36. A method of displaying one or more packet properties or statistics on a  
2 display device having a display area, the one or more packet properties or statistics  
3 corresponding to packets received from a first communication line during an interval of  
4 time, the method comprising:

5 (a) displaying a table listing the one or more packet properties or statistics in a  
6 first portion of the display area; and

7 (b) displaying a plot of the one or more packet properties or statistics over the  
8 time interval in a second portion of the display area, the plot having two axes, the packet  
9 properties or statistics being represented on one axis of the plot, and time represented on  
10 the other axis of the plot.

1 37. The method according to claim 36 wherein the packets correspond to a  
2 plurality of protocols at a protocol layer wherein step (a) includes displaying a table listing  
3 each of the plurality of protocols and a corresponding number of packets.

1 38. The method according to claim 37, further comprising the steps of detecting  
2 selection of one of the plurality of protocols and updating at least one of the table to  
3 display packet properties corresponding to packets of the selected protocol and the plot to  
4 display a packet properties of the selected protocol .

1 39. The method according to claim 36 further comprising the steps of:  
2 receiving a selection of a sub-interval of time less than the interval of time by one  
3 of entry of times in a text field and selection of a time interval along the time axis of the  
4 plot; and

5 updating at least one of the tables and the plots responsive to the selected sub-  
6 interval of time.

1 40. The method according to claim 37, further comprising the steps of detecting  
2 selection of one of the plurality of protocols and updating the plot to simultaneously  
3 display both the packet properties of the selected protocol and the packet properties of all  
4 protocols.

1           41.     The method according to claim 36 further comprising the steps of receiving  
2 a start time and an end time spanning a duration longer than the time interval and updating  
3 at least one of the tables and the plots to correspond to the duration.

1           42.     The method according to claim 36 wherein a subset of the packets  
2 correspond to a host and the method further comprises detecting selection of the host and  
3 displaying statistics corresponding to the subset of packets.

1           43.     The method according to claim 36 wherein the packets correspond to a  
2 plurality of protocols and a subset of the packets correspond to one of the plurality of the  
3 protocols and the method further comprises detecting selection of the one of the plurality  
4 of the protocols and displaying statistics corresponding to the selected one of the plurality  
5 of protocols.

1           44.     A method of synchronizing a host clock on a host computer with an  
2 interface clock on a network interface card comprising the steps of:  
3           receiving an interface clock value from the network interface card;  
4           generating an adjusted interface clock value by subtracting a predetermined service  
5 time from the interface clock value ;  
6           providing the adjusted interface clock value to the host computer;  
7           receiving a host clock value;  
8           correlating the adjusted interface clock value with the host clock value.

1           45.     A method of monitoring communications on a network having a first  
2 communication line and a second communication line different from the first  
3 communication line, the method comprising the steps of:

- 4           (a)     receiving a first plurality of packets from the first communication line;  
5           (b)     receiving a second plurality of packets from the second communication  
6 line; and  
7           (c)     correlating the first plurality and the second plurality of packets.



1           46.    The method according to claim 45 wherein step (c) includes extracting a  
2 uniquely identifying portion of each of the first plurality and second plurality of packets  
3 and comparing the uniquely identifying portions of the first plurality of packets to those of  
4 the second plurality of packets to generate matched pairs of packets.

1           47.    The method according to claim 45 wherein the first plurality of packets are  
2 received by a first network monitor, the second plurality of packets are received by a  
3 second network monitor, step (a) includes time stamping the first plurality of packets, step  
4 (b) includes time stamping the second plurality of packets, and the method further  
5 comprises the step of synchronizing the first and second network monitors with an  
6 absolute clock reference.

1           48.    The method according to claim 47 wherein the network monitors are  
2 synchronized by receiving a time signal from a global positioning satellite.

1           49.    A system for monitoring communication on a network including a first  
2 communication line and a second communication line, the system comprising:

3           a first network monitor having a first clock and coupled to the first communication  
4 line for receiving first data from the first communication line;

5           a second network monitor having a second clock and coupled to the second  
6 communication line for receiving second data from the second communication line;

7           synchronizing means for synchronizing the first clock with the second clock.

1           50.    A system according to claim 49 wherein the first clock and the second  
2 clock are synchronized within one microsecond of each other.

1           51.    A system according to claim 49 wherein the synchronizing means  
2 comprises:

3           a receiver associated with the first network monitor for receiving a time signal  
4 from a common clock reference; and

5           a receiver associated with the second network monitor for receiving a time signal  
6 from the common clock reference.

09563593-052301  
T052301-052301

1           52.     A system according to claim 51 wherein the common clock reference is a  
2 global positioning satellite system.

1           53.     A method for billing a user of a communication network comprising steps  
2 of:

3           determining a quality of service metric corresponding to the user's use of the  
4 communication network;

5           billing the user based on the determined quality of service.

1           54.     A method of transmitting data onto a communication line comprising the  
2 steps of:

3           associating a time with the data;

4           generating a packet including a plurality of fields, wherein at least one field  
5 corresponds to the associated time and at least one field corresponds to the data;

6           transmitting the packet onto the communication line.

1           55.     An apparatus for transmitting data onto a communication line comprising:

2           a clock for providing a time value corresponding to the data;

3           an encoder for encoding a packet, the packet including a plurality of fields, wherein  
4 at least one field corresponds to the time value and at least one field corresponds to the  
5 data;

6           a transmitter for providing the packet to a communication line.

1           56.     A system for monitoring a computer network over an interval of time, in  
2 which data packets travel across network paths during such time interval, the system  
3 comprising:

4           means for recording the packets substantially continuously during the time interval;

5           means for extracting packet properties from the recorded packets at multiple,  
6 successive sampling times during said time interval, the time from the beginning of the  
7 time interval to successive sampling times defining subintervals of time during which the  
8 network has been monitored, the subintervals being increasingly longer as packet  
9 properties are extracted over successive sampling times during the time interval;

09063593-052301

means for tabulating the extracted packet properties for the subintervals to create statistical information;

means for altering the recording of the packets and the extraction of packet properties in response to user selections;

means for creating, during the time interval, data corresponding to graphical representations of the statistical information in response to the creation of the statistical information;

means for displaying said graphical representations in response to the creation of said graphical representations.

57. The system of claim 56, wherein the recording means includes:  
means for detecting the packets travelling over a selected one of the network paths;  
means for indexing the detected packets;  
means for creating records corresponding to the packets; and  
means for storing the records in memory.

58. The system of claim 57, wherein the detecting means includes means for determining packet properties and means for selecting certain ones of the data packets traveling the network path and having a predetermined packet property.

59. The system of claim 57, wherein the indexing means comprises means for timestamping the data packets.

60. The system of claim 59, in which the network is monitored at two points on the network, the system further comprising timestamping means at the two points, and wherein the timestamping means comprises GPS means for synchronizing the indexing of the data packets at the two points.

61. The system of claim 57 further comprising a computer with a data storage device, a network card having network card memory, and a CPU in logical communication with the network card, and wherein the record storing means comprises:  
means for storing the records on the network card memory;  
means for detecting relative inactivity of the CPU; and

means for transferring records stored on the network card memory to the data storage device in response to detection of the relative inactivity of the CPU.

62. The system of claim 61, wherein the record storing means further comprises:

a long-term storage device having replaceable storage media loaded therein so as to receive data thereon, and a magazine of additional storage media operatively connected to the long-term storage device;

means for detecting when the data storage device of the computer contains a predetermined amount of data corresponding to the recorded packets, said predetermined amount of data corresponding to the data storage device being full;

means for transferring said data from the data storage device to the long-term storage device in response to detecting the data storage device is full;

means for detecting when the replaceable media loaded in the long-term storage device is full; and

means for replacing the full storage media with storage media from the magazine.

63. The system of claim 56, wherein the displaying means includes a computer display screen having a graphical user interface and a control program for the graphical user interface, the control program having:

means for displaying at least some of the packet properties over time on a graph having two axes, the packet properties being represented on one axis of the graph, the time being represented on the other axis of the graph;

means for varying the timescale of the graph in response to user selection; and

means for displaying at least some of the statistical information in at least one table adjacent to the graph, the tables having user-selectable cells therein; and

means, responsive to selection of one of the cells, for displaying additional statistical information corresponding to the selected cell.

64. A system for monitoring data on a first communication line comprising:

a packetizer for receiving the data from the first communication line and extracting a plurality of packets from the data; and

means for recursively generating statistics corresponding to the plurality of packets.

65. A system according to claim 64 wherein the means for recursively generating statistics comprises:

- means for generating records corresponding to the plurality of packets;
- a filter for selecting packets from the plurality of packets received by the system during a time period;
- means for generating first statistics corresponding to the plurality of packets received by the system during the time period;
- a memory for storing at least one of the selected packets, the records corresponding to the plurality of packets, and the first statistics;
- a packet type identifier for identifying a type of packets received from one of the packetizer, the record generator, and the memory;
- means for generating second statistics using at least one of the first statistics and the received packets.

66. A system according to claim 64 further comprising a display device for displaying the generated statistics.

67. A system according to claim 65 further comprising a user interface for defining at least one of the first statistics, the second statistics, and the time period.

68. A system according to claim 65 further comprising:

- a time source synchronized to an absolute time source; and
- means for determining a time when each respective one of the plurality of packets was received from the first communication line.

69. A system according to claim 68 wherein the time source is a receiver for receiving a time signal from a global positioning satellite.

70. An article of manufacture comprising a computer useable medium having computer readable program code means embodied therein for monitoring data on a first communication line, the computer readable program code means in said article of manufacture comprising computer readable program code means for causing a computer to effect:

- receiving the data from the first communication line;
- extracting a plurality of packets from the received data; and
- recursively generating statistics corresponding to the plurality of packets.

1 71. A computer program product comprising a computer useable medium  
2 having computer readable program code means embodied therein for monitoring data on a  
3 first communication line, said computer readable program code means in said computer  
4 program product comprising computer readable program code means for causing a  
5 computer to effect:receiving the data from the first communication line;

6 extracting a plurality of packets from the received data; and  
7 recursively generating statistics corresponding to the plurality of packets.

1 72. A program storage device readable by machine, tangibly embodying a  
2 program of instructions executable by the machine to perform method steps for monitoring  
3 data on a first communication line, said method steps comprising:

4 receiving the data from the first communication line;  
5 extracting a plurality of packets from the received data; and  
6 recursively generating statistics corresponding to the plurality of packets.

1 73. An article of manufacture comprising a computer useable medium having  
2 computer readable program code means embodied therein for displaying packet properties  
3 on a display device having a display area, the packet properties corresponding to packets  
4 received from a first communication line during an interval of time, the computer readable  
5 program code means in said article of manufacture comprising computer readable program  
6 code means for causing a computer to effect:

7 (a) displaying a table listing the packet properties in a first portion of the  
8 display area; and

9 (b) displaying a plot of the packet properties over the time interval in a second  
10 portion of the display area, the plot having two axes, the packet properties being  
11 represented on one axis of the plot, and time represented on the other axis of the plot.

1 74. A computer program product comprising a computer useable medium  
2 having computer readable program code means embodied therein for causing displaying  
3 packet properties on a display device having a display area, the packet properties  
4 corresponding to packets received from a first communication line during an interval of  
5 time, said computer readable program code means in said computer program product  
6 comprising computer readable program code means for causing a computer to effect:(a)

7 displaying a table listing the packet properties in a first portion of the display area;  
8 and

9 (b) displaying a plot of the packet properties over the time interval in a second  
10 portion of the display area, the plot having two axes, the packet properties being  
11 represented on one axis of the plot, and time represented on the other axis of the plot.

1 75. A program storage device readable by machine, tangibly embodying a  
2 program of instructions executable by the machine to perform method steps for displaying  
3 packet properties on a display device having a display area, the packet properties  
4 corresponding to packets received from a first communication line during an interval of  
5 time, said method steps comprising:

6 (a) displaying a table listing the packet properties in a first portion of the  
7 display area; and

8 (b) displaying a plot of the packet properties over the time interval in a second  
9 portion of the display area, the plot having two axes, the packet properties being  
10 represented on one axis of the plot, and time represented on the other axis of the plot.

1 76. An article of manufacture comprising a computer useable medium having  
2 computer readable program code means embodied therein for collecting and analyzing first  
3 data transmitted on a first communication line, the computer readable program code means  
4 in said article of manufacture comprising computer readable program code means for  
5 causing a computer to effect:

6 (a) receiving the first data from the first communication line;

7 (b) segregating the received first data into packets;

8 (c) determining a respective type of each packet;

9 (d) selecting packets based on their respective type;

10 (e) associating a respective index with each of the selected packets;

11 (f) converting each of the selected packets into a respective record including its  
12 respective index;

13 (g) storing the records in a first memory;

14 (h) receiving a first duration value corresponding to a first time period;

15 (i) generating at least one statistic corresponding to packets received during each  
16 successive time period; and

17 (j) storing the at least one statistic for each successive time period in a second  
18 memory.

1 77. A computer program product comprising a computer useable medium  
2 having computer readable program code means embodied therein for collecting and  
3 analyzing first data transmitted on a first communication line, said computer readable  
4 program code means in said computer program product comprising computer readable  
5 program code means for causing a computer to effect:

6 (a) receiving the first data from the first communication line;  
7 (b) segregating the received first data into packets;  
8 (c) determining a respective type of each packet;  
9 (d) selecting packets based on their respective type;  
10 (e) associating a respective index with each of the selected packets;  
11 (f) converting each of the selected packets into a respective record including its  
12 respective index;

13 (g) storing the records in a first memory;  
14 (h) receiving a first duration value corresponding to a first time period;  
15 (i) generating at least one statistic corresponding to packets received during each  
16 successive time period; and  
17 (j) storing the at least one statistic for each successive time period in a second  
18 memory.

1 78. A program storage device readable by machine, tangibly embodying a  
2 program of instructions executable by the machine to perform method steps for collecting  
3 and analyzing first data transmitted on a first communication line, said method steps  
4 comprising:

5 (a) receiving the first data from the first communication line;  
6 (b) segregating the received first data into packets;  
7 (c) determining a respective type of each packet;  
8 (d) selecting packets based on their respective type;  
9 (e) associating a respective index with each of the selected packets;



10 (f) converting each of the selected packets into a respective record including its  
11 respective index;  
12 (g) storing the records in a first memory;  
13 (h) receiving a first duration value corresponding to a first time period;  
14 (i) generating at least one statistic corresponding to packets received during each  
15 successive time period; and  
16 (j) storing the at least one statistic for each successive time period in a second  
17 memory.

79. A method according to claim 3, further comprising the steps of:

(l) selecting packets corresponding to particular communication sessions; and

(m) identifying which of the packets selected in step (l) correspond to  
unsuccessful communication sessions.

80. A method for processing data according to claim 79 wherein:

step (l) comprises selecting packets corresponding to TCP sessions; and

step (m) comprises identifying packets corresponding to unsuccessful TCP  
sessions; and the method further comprise the step of:

(n) generating a ratio of a quantity of unsuccessful TCP sessions to a quantity  
of total TCP sessions during a time period.

81. A method according to claim 80 wherein in step (m) the unsuccessful TCP  
sessions are identified to be those TCP sessions that were closed by other than a  
corresponding server.